REMARKS

Claims 1 – 4, 6 and 12 are cancelled. The remaining pending claims were rejected under 35 U.S.C. 103(a) as being unpatentable over High-bandwidth Digital Content Protection System, Revision 1.0 by Intel Corporation (HDCP Revision 1) in view of Matyas reference discussed previously.

Upon thorough consideration of both references, the Applicants believe that new claims 23 and 25 traverse the Examiner's obviousness type rejection for at least the following reasons. In neither reference, is there any indication whatsoever that a first decryption key (formed by applying a first encryption protocol on a first encrypted key) once used to decrypt an encrypted display signal is destroyed to be replaced by a second decryption key formed by applying a second encryption protocol on a second encryption key, where the first and the second encryption protocols are different. This is evident in the HDCP reference starting on page 6,first paragraph describing the authentication protocol and more particularly, in section 2.1 Overview, "Each authorized participant...receives an array of 40, 56 bit secret device keys and a corresponding identifier from the Digital Content Protection LLC. **This identifier is the Key Selection Vector (KSV) assigned to the device**. " (emphasis added) Therefore, since the KSV is assigned to the device, it **never** changes and therefore is subject o hacking.

Unfortunately, maintaining a constant KSV that was assigned to the device, the HDCP system is susceptible to "hacking" if that single assigned KSV is compromised. This general shortcoming of the prior art is described in the specification at page 12, first full paragraph:

> One problem with the above embodiment is that an unauthorized third party may retrieve the encrypted key multiple times and attempt to decipher the unencrypted key. To discourage such attempts, support for multiple encryption/decryption protocols (for encrypting the keys) may be provided within integrated circuit 201, and the keys may be encrypted according to one of the protocols. The OEM may specify the specific protocol by using appropriate commands. The data indicating the specific protocol may also be stored thereafter in serial EEPROM 250 to facilitate later decryption by HDCP engine 290.

Therefore, the invention solves this problem by providing for destroying an already used decryption key to be replaced by another decryption key using a totally different encryption protocol thereby rendering the system invulnerable to hacking. In particular, claim 1 recites:

> " retrieving a first encrypted key from a non-volatile memory incorporated in the display unit;
> generating a first decrypted key by decrypting the first encrypted key according to a first encryption protocol;
> receiving a plurality of pixel data elements encoded in a display signal in an encrypted form that represent an image;
> decrypting said encrypted plurality of pixel data elements using the first decrypted key;
> generating said plurality of pixel data elements based upon said decrypted plurality of pixel data elements;
> displaying said image on a display screen based on said decrypted plurality of pixel data elements;
> destroying the first encrypted key;
> receiving a second encrypted key from the non-volatile memory that is different from the first encrypted key;
> generating a second decrypted key by decrypting the second encrypted key according to a second encryption protocol that is different from the first encryption protocol; and
> decrypting said encrypted plurality of pixel data elements using the second decrypted key".

In this way, the invention provides an additional layer of security since each key may in fact have been encrypted by a separate and different encryption protocol therefore preventing the shortcoming of encrypting all the cryptographic keys with the same encryption protocol as is done with both the HDCP and Matyas references.

Therefore, the Applicants believe that neither of the cited references taken singly or in any combination render the invention as recited in claim 23 unpatentable and respectfully request that the Examiner withdraw the U.S.C. 103(a) rejection of claim 23 and all claims dependent thereon.

Independent claim 25 recites the same limitation as does claim 23 and therefore the Applicants also believe that claim 25 and all claims dependent thereon are allowable for at least the same reasons stated above for claim 23.

CONCLUSION

In view of the foregoing, it is respectfully submitted that all pending claims are allowable. Should the Examiner believe that a further telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,

BEYER WEAVER & THOMAS, LLP

/Michael J. Ferrazano/
Michael J. Ferrazano
Reg. No. 44,105

P.O. Box 70250
Oakland, CA 94612-0250
(650) 961-8300